UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,975	02/04/2002	Michael J. Wookey	P7235	4232

33438 7590 08/24/2006

HAMILTON & TERRILE, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,975	WOOKEY ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/20/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are pending.

2. In view of the Appeal filed on February 22, 2005, PROSECUTION IS HEREBY REOPENED. The Non-Final rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 10-11, and 13-16 are rejected under 35 U.S.C. 102(e) as being anticipated by, et Britt, Jr. et al. (US 6,230,319).

As per claim 1:

Britt, Jr. et al. discloses a method of automatically reconfiguring a component of a remote services network system comprising the steps of:

detecting a communication error related to a component of said network; **[col.8, lines 15-16]**

identifying a configuration parameter associated with the occurrence of said communication error; **[col.8, lines 26-30; Britt, Jr. discloses validating contents which includes various (data) configuration parameters (col.7, lines 50-53) where if these contents are corrupted or inconsistent state, then it is associated to communication error.]**

obtaining corrected configuration data relating to said configuration parameter; and **[col.8, lines 32-33]**

automatically installing said corrected configuration data on said component **[col.8, lines 35-39]** to restore communication with said remote services network. **[col.11, lines 41-44 and col.12, lines 25-35]**

As per claim 2: **See col.8, lines 26-30;** discussing communication error comprising an error in the identity of said component.

As per claim 3: **See col.11, lines 41-44 and col.12, lines 25-35;** discussing communication error comprising an error related to connectivity of said component to said remote services network.

As per claim 10:

Britt discloses a remote services system, comprising:

a system component in communication with said remote services system, **[col.4, lines 32-41 and col.6, lines 58-61]** said component having a plurality of stored data parameters for maintaining communication with said remote services system; **[col.7, lines 51-55]**

a data base containing valid configuration data parameters for maintaining communication of said system component with said remote services system; and **[col.7, lines 31-36]**

a communication module operable to detect a communication error between said system component and said remote services system **[col.11, lines 41-44]** and to correct said communication error **[col.8, lines 15-16 and 26-30; Britt, Jr. discloses validating contents which includes various (data) configuration parameters (col.7, lines 50-53) where if these contents are corrupted or inconsistent state, then it is**

associated to communication error.] by obtaining valid configuration data parameters from said data base **[col.8, lines 32-33]** and installing said valid configuration data parameters on said system component. **[col.8, lines 35-39]**

As per claim 11: **See col.8, lines 26-30;** discussing communication error comprises an error in the identity of said component.

As per claim 13: **See col.8, lines 15-16 and 26-30 and col.11, lines 41-44;** discussing communication error comprises an error related to connectivity of said component to said remote services network.

As per claim 14: **See col.7, lines 31-36 and col.9, lines 9-21;** discussing an application server, said application server being operable to obtain valid configuration data parameters from said data base and to transmit said valid configuration data parameters to said system component in response to an instruction received from said communication module.

As per claim 15: **See col.7, lines 31-36;** discussing database residing on a server controlled by a service provider.

As per claim 16: **See col.10, lines 51-61;** discussing a internet web site for providing limited access to said data base residing on said server controlled by said service provider.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4-9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Britt, Jr. et al. (US 6,230,319), and further in view of Howard, Jr. et al. (US 6,442,690).

As per claim 4:

Britt, Jr. et al. discloses a method of automatically reconfiguring a component of a remote services network system comprising detecting a communication error related to a component of said network [col.8, lines 15-16] and identifying a configuration parameter associated with the occurrence of said communication error [col.8, lines 26-30]. Britt, Jr. discloses validating contents which includes various (data) configuration parameters where if these contents are corrupted or inconsistent state, then it is associated to communication error (col.7, lines 50-53). Further, Britt, Jr. discloses obtaining corrected configuration data relating to said configuration parameter [col.8, lines 32-33] and automatically installing said corrected configuration data on said component [col.8, lines 35-39] to restore communication with said remote services

network. [col.11, lines 41-44 and col.12, lines 25-35]. However, Britt, Jr. fails to include a client certificate.

Howard, Jr. et al. discloses an integrated key management system that can support key generation and key distribution for numerous types of equipment (col.6, lines 1-2). Howard discloses IKMS can provide secure storage of key material and can allow for key recovery during disasters, equipment failure, etc., where it can support secure automated distribution of keys to equipment and rapid redistribution of previously distributed key material to restore secure communications services (col.6, lines 14-20). Howard discusses the View Key Inventory function that allows an operator to list all key material held securely in the IKMS database (col.19, lines 6-9) and the View Network Connectivity function lists the communication relationship defined within IKMS and show the type of cryptographic protection provided by this communication relationship (col.19, lines 19-23). There also includes a CPE error indicator at the bottom of the IKMS desktop where this can show communications error (col.16, lines 13-19 and col.19, lines 54-56). Howard discloses IKMS communicates with the device over open networks and exchanges certificate information where verification ensures that this is the first time the certificate has been used and the identity of the device (col.10, lines 6-15 and col.23, lines 61-67). Howard discloses the certificate is provided the IKMS over the public network where the certificate is validated, verifies the device ID, and the certificate are associated (col.26, lines 13-32). Therefore, it would have been obvious for a person of ordinary skills in the art to include a certificate as taught by Howard, Jr. with the teaching of automatically reconfiguring a component of a remote services network

system as taught by Britt, Jr. because the certificate authenticates and verifies the device and its communications.

As per claim 5:

Britt, Jr. discloses the step of obtaining corrected configuration data further comprising the step of requesting a valid client [certificate] from a secure universal resource locator associated with a service provider web site containing data parameters relating to components of said remote services system **[col.8, lines 32-33 and col.10, lines 51-61]**. However, Britt, Jr. fails to include a certificate.

Howard, Jr. et al. discloses an integrated key management system that can support key generation and key distribution for numerous types of equipment (col.6, lines 1-2). Howard discloses IKMS can provide secure storage of key material and can allow for key recovery during disasters, equipment failure, etc., where it can support secure automated distribution of keys to equipment and rapid redistribution of previously distributed key material to restore secure communications services (col.6, lines 14-20). Howard discusses the View Key Inventory function that allows an operator to list all key material held securely in the IKMS database (col.19, lines 6-9) and the View Network Connectivity function lists the communication relationship defined within IKMS and show the type of cryptographic protection provided by this communication relationship (col.19, lines 19-23). There also includes a CPE error indicator at the bottom of the IKMS desktop where this can show communications error (col.16, lines 13-19 and col.19, lines 54-56). Howard discloses IKMS communicates with the device over open networks and exchanges certificate information where verification ensures that this is the first time the

certificate has been used and the identity of the device (col.10, lines 6-15 and col.23, lines 61-67). Howard discloses the certificate is provided the IKMS over the public network where the certificate is validated, verifies the device ID, and the certificate are associated (col.26, lines 13-32). Therefore, it would have been obvious for a person of ordinary skills in the art to include a certificate as taught by Howard, Jr. with the teaching of automatically reconfiguring a component of a remote services network system as taught by Britt, Jr. because the certificate authenticates and verifies the device and its communications.

As per claim 6: **as rejected in claim 4.**

As per claim 7: **See Britt, Jr. on col.12, lines 25-35;** discussing the step of revalidating communications of said component with said remote services system.

As per claim 8: **as rejected in claim 5**

As per claim 9: **See Britt, Jr. on col.12, lines 25-35;** discussing the step of revalidating communications of said component with said remote services system.

As per claim 12:

Britt, Jr. et al. discloses a method of automatically reconfiguring a component of a remote services network system comprising detecting a communication error related to a component of said network [col.8, lines 15-16] and identifying a configuration parameter associated with the occurrence of said communication error [col.8, lines 26-30]. Britt, Jr. discloses validating contents which includes various (data) configuration

parameters where if these contents are corrupted or inconsistent state, then it is associated to communication error (col.7, lines 50-53). Further, Britt, Jr. discloses obtaining corrected configuration data relating to said configuration parameter [col.8, lines 32-33] and automatically installing said corrected configuration data on said component [col.8, lines 35-39] to restore communication with said remote services network. [col.11, lines 41-44 and col.12, lines 25-35]. However, Britt, Jr. fails to include a client certificate.

Howard, Jr. et al. discloses an integrated key management system that can support key generation and key distribution for numerous types of equipment (col.6, lines 1-2). Howard discloses IKMS can provide secure storage of key material and can allow for key recovery during disasters, equipment failure, etc., where it can support secure automated distribution of keys to equipment and rapid redistribution of previously distributed key material to restore secure communications services (col.6, lines 14-20). Howard discusses the View Key Inventory function that allows an operator to list all key material held securely in the IKMS database (col.19, lines 6-9) and the View Network Connectivity function lists the communication relationship defined within IKMS and show the type of cryptographic protection provided by this communication relationship (col.19, lines 19-23). There also includes a CPE error indicator at the bottom of the IKMS desktop where this can show communications error (col.16, lines 13-19 and col.19, lines 54-56). Howard discloses IKMS communicates with the device over open networks and exchanges certificate information where verification ensures that this is the first time the certificate has been used and the identity of the device (col.10, lines 6-15 and col.23,

lines 61-67). Howard discloses the certificate is provided the IKMS over the public network where the certificate is validated, verifies the device ID, and the certificate are associated (col.26, lines 13-32). Therefore, it would have been obvious for a person of ordinary skills in the art to include a certificate as taught by Howard, Jr. with the teaching of automatically reconfiguring a component of a remote services network system as taught by Britt, Jr. because the certificate authenticates and verifies the device and its communications.

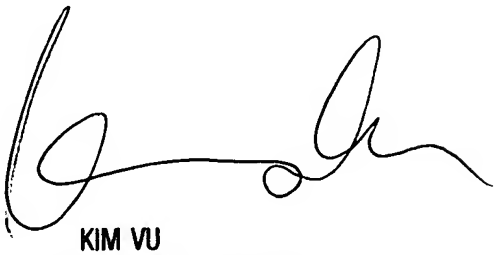
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100